



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/646,398	08/21/2003	Eric J. Sprunk	018926-010010US	9498
7590 Robert P. Marley Motorola, Inc. Broadband Communications Sector 101 Tournament Drive Horsham, PA 19044	04/18/2007		EXAMINER REZA, MOHAMMAD W	ART UNIT 2136 PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE		
3 MONTHS	04/18/2007	PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/646,398	SPRUNK, ERIC J.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Mohammad W. Reza	2136	

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 31 January 2007.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-9, 11-15, 17-19 and 21-31 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-9, 11-15, 17-19, and 21-31 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to..  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |  |
|---|--|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)            |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                        | Paper No(s)/Mail Date. _____                                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____. | 5) <input type="checkbox"/> Notice of Informal Patent Application. |
|   | 6) <input type="checkbox"/> Other: _____.                          |

Art Unit: 2136

**DETAILED ACTION**

1. This is in response to the arguments filed on 01/31/2008.
2. Claims 1-9, 11-15, 17-19, and 21-31 are pending in the application.
3. Claims 1-9, 11-15, 17-19, and 21-31 have been rejected.

*Response to Amendment*

4. The examiner approves the amendments made to claims 1, 2, 12, 13, and 18.
5. The examiner approves cancellation of claims 10, 16, and 20.
6. The examiner withdraws the 101 rejection regarding claims 10, 16, and 20 as those claims are cancelled.

*Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In these claims applicants mentioned, "encrypting first content using a first method that is cryptographically secured with second decryption information" which is generally narrative and indefinite with the invention. Applicants do not point out clearly which options include in the present invention by encrypting first content using a first method that is cryptographically secured with second decryption information and how these steps perform in the invention. In support

of “**a first method**” examiner only able to find in one place in specification where applicant mention about it but irrelevant with the present claim limitations. “A first program is encrypted using a first method that is cryptographically related to second decryption information (abstract)” which does not reflect the limitations as cited in the claim and what does it mean by **“a first method”**. The office will interpret these limitations with the regarding claims as best understood for applying the appropriate art for rejection purposes.

### ***Response to Arguments***

8. Applicant's arguments filed on 01/31/2007 have been fully considered but they are not persuasive.

Applicant argues, “distributing the second decryption key information which is received by the receivers from the broadcaster (transmitter)” does not teach by Bowman.

Applicants also argues that the second decryption information in Bowman actually generated by receiver. Examiner respectfully disagrees, for example, “The method comprises a first step of performing a first predefined algorithm at the transmitter station to generate Subscription Key values for the respective authorized receiver stations (col. 1, lines 62-65)”, “A next step includes providing the generated Subscription Key values to the respective authorized receiver stations. In accordance with one embodiment of the invention, the Subscription Key values may be provided to the authorized receiver stations by way of an information signal transmitted from the transmitter station. In other embodiments of the invention, the Subscription Key values may be provided directly to

Art Unit: 2136

users of the authorized receiver stations, in which case the users then enter these values into the respective authorized receiver stations using a suitable user-interface (col. 2, lines 9-18)", "In one embodiment, when a S-Key value is provided to an authorized receiver station (A-D), the Tag value corresponding to the S-Key value is also provided to the authorized receiver station (A-D), as will be further described below (col. 6, lines 53-56)", and "...receiver station 2a receiving the S-key value from transmitter station 6 (col. 7, lines 45-46)" discloses that decryption information actually provides by transmitter.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-9, 11-15, 17-19, and 21-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Bowman et al hereafter Bowman (US patent 5999623).
10. As per claim 1, Bowman discloses a method comprising steps of: at a broadcaster: receiving provisioning information from a subset of the population of digital receivers indicating that the subset is potentially within range to receive digital television from a broadcaster (col. 1, lines 12-22); distributing first decryption information to the subset of the population of digital receivers (col. 1, lines 56-67, col. 2, lines 1-19, col. 6,

lines 23-48), wherein: the first decryption information allows for potentially decrypting a plurality of programs coextensively in time (col. 2, lines 25-36), and the unauthorized digital receivers are cryptographically excluded from using the first decryption information (col. 1, lines 26-42, col. 6, lines 23-48, col. 17, lines 62-67); encrypting first content using a first method that is cryptographically secured with second decryption information; sending the first content (col. 14, lines 43-67, col. 19, lines 38-59); and distributing the second decryption information to the subset of the population of digital receivers, wherein the second decryption information is cryptographically secured with the first decryption information (col. 6, lines 22-48, col. Col. 18, lines 9-36).

11. As per claim 2, Bowman discloses the method comprising steps of: encrypting second content using a second method that is cryptographically related to third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method (col. 14, lines 43-67, col. 19, lines 38-59); sending the second content; and distributing third decryption information to the subset of the population of digital receivers, wherein the second decryption information is cryptographically secured with the first decryption information (col. 6, lines 22-48, col. Col. 18, lines 9-36).

12. As per claim 3, Bowman discloses the method comprising a step of uniquely encrypting the first decryption information for each of the subset, wherein the first-listed distributing step comprises sending first description information uniquely encrypted for each of the subset (col. 14, lines 43-67, col. 19, lines 38-59).

Art Unit: 2136

13. As per claim 4, Bowman discloses the method comprising a step of determining the unauthorized digital receivers to exclude from the subset of the population of digital receivers (col. 1, lines 26-42, col. 6, lines 23-48, col. 17, lines 62-67).

14. As per claim 5, Bowman discloses the method, wherein the first decryption information is uniquely encrypted for each of the subset (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

15. As per claim 6, Bowman discloses the method wherein the first decryption information comprises a key for decrypting the second decryption information (col. 14, lines 43-67, col. 19, lines 38-59).

16. As per claim 7, Bowman discloses the method, wherein the first decryption information expires by changing keys, key lengths and/or algorithms used to encrypt the first content (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

17. As per claim 8, Bowman discloses the method comprising a step of forwarding the provisioning information to another broadcaster within range of one of the subset (col. 1, lines 12-22).

18. As per claim 9, Bowman discloses the method, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the unique identifier includes a key (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

19. As per claim 11, Bowman discloses a computer-readable medium protecting television from unauthorized digital receivers within the population of digital receivers of claim 1, and method for protecting digital television from unauthorized digital receivers within the population of digital receivers of claim 1.

Art Unit: 2136

20. As per claim 12, Bowman discloses a method comprising steps of: sending provisioning information from a subset of the population of digital receivers indicating that the subset is within range to receive digital television from a broadcaster (col. 1, lines 12-22); receiving first decryption information with the subset of the population of digital receivers (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48), wherein: the first decryption information allows for potentially decrypting a plurality of programs coextensively in time (col. 2, lines 25-36), and the unauthorized digital receivers are cryptographically excluded from using the first decryption information (col. 1, lines 26-42, col. 6, lines 23-48, col. 17, lines 62-67); receiving first content; receiving second decryption information that is cryptographically secured with the first decryption information (col. 6, lines 22-48, col. Col. 18, lines 9-36); and decrypting the first content using a first method that is cryptographically related to the second decryption information (col. 14, lines 43-67, col. 19, lines 38-59).

21. As per claim 13, Bowman discloses the method comprising steps of: receiving second content; receiving third decryption information that is cryptographically secured with the first decryption information (col. 6, lines 22-48, col. Col. 18, lines 9-36); and decrypting the second content using a second method that is cryptographically related to the third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method (col. 14, lines 43-67, col. 19, lines 38-59).

22. As per claim 14, Bowman discloses the method, where each digital receiver in the population has the unique identifier as recited in claim 12, wherein the first

decryption information is uniquely encrypted for each of the subset (col. 14, lines 43-67, col. 19, lines 38-59).

23. As per claim 15, Bowman discloses the method, where each digital receiver in the population has the unique identifier as recited in claim 12, wherein the unique identifier includes a key (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

24. As per claim 17, Bowman discloses a computer-readable medium for processing digital television within the population of digital receivers of claim and a computer system adapted to perform the computer-implementable method for processing digital television within the population of digital receivers of claim 12 (col. 1, lines 12-22).

25. As per claim 18, Bowman discloses a method comprising steps of: at a broadcaster: determining a first subset of the population of digital receivers, wherein the first subset is within range to receive digital television from a broadcaster (col. 1, lines 12-22); distributing first decryption information to the first subset of the population of digital receivers (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48), wherein: the first decryption information is uniquely encrypted for each of the first subset (col. 2, lines 25-36), and the first decryption information expires at some future time; encrypting first content that is cryptographically protected from use by digital receivers without the first decryption information (col. 1, lines 26-42, col. 6, lines 23-48, col. 17, lines 62-67); sending the first content in encrypted form; determining the unauthorized digital receivers to exclude from the first subset to find a second subset of the population of digital receivers, and sending the second content in encrypted form after the first decryption information has expired (col. 6, lines 22-48, col. Col. 18, lines 9-36);

Art Unit: 2136

distributing second decryption information to the second subset of the population of digital receivers, wherein the second decryption information is uniquely encrypted for each of the second subset (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48); encrypting second content that is cryptographically protected from use by digital receivers without the second decryption information (col. 14, lines 43-67, col. 19, lines 38-59).

26. As per claim 19, Bowman discloses the method, wherein the first and second decryption information assists in decrypting messages with keys that allow decrypting the first content (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

27. As per claim 21, Bowman discloses a computer-readable medium for protecting digital television from unauthorized digital receivers within the population of digital receivers of claim 18, and a computer system for protecting digital television from unauthorized digital receivers within the population of digital receivers of claim 18 (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

28. As per claim 22, Bowman discloses a content receiver comprising: provisioning information that is sent away from the content receiver for a plurality of content broadcasters coupled to the content receiver (col. 1, lines 12-22); first decryption information received from a point remote to the content receiver, wherein an unauthorized content receiver is excluded from using the first decryption information (col. 1, lines 26-42, col. 6, lines 23-48, col. 17, lines 62-67); an interface coupled to content signals broadcast to a plurality of content receivers, wherein the content signals carry a plurality of programs coextensively in time (col. 2, lines 25-36); second

Art Unit: 2136

decryption information received from a place remote to the content receiver, wherein the second decryption information is cryptographically secured with the first decryption information (col. 14, lines 43-67, col. 19, lines 38-59); and first content received with the interface, wherein the first content is decrypted with a method related to the second decryption information (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

29. As per claim 23, Bowman discloses the content receiver, wherein the content signals are protected by a plurality of encryption keys (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

30. As per claim 24, Bowman discloses the content receiver, wherein the first decryption information includes a category key (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

31. As per claim 25, Bowman discloses the content receiver, wherein the first decryption information includes a category key (col. 2, lines 25-36).

32. As per claim 26, Bowman discloses the content receiver, wherein the second decryption information includes a content key (col. 1, lines 12-22).

33. As per claim 27, Bowman discloses the content receiver, wherein the first decryption information expires after a period of time (col. 6, lines 22-48, col. Col. 18, lines 9-36).

34. As per claim 28, Bowman discloses the content receiver for protecting content that is transmitted with digital encoding as recited in claim 27, wherein the period of time is two hours, one day, one week, one month, or one year (col. 6, lines 22-48, col. Col. 18, lines 9-36).

Art Unit: 2136

35. As per claim 29, Bowman discloses the content receiver, wherein the first decryption information is uniquely encrypted for each of a plurality of content receivers in a system (col. 1, lines 26-42, col. 6, lines 23-48, col. 17, lines 62-67).

36. As per claim 30, Bowman discloses the content receiver comprising a plurality of content keys, wherein the first content is protected with one of the plurality of content keys (col. 1, lines 56-67, col. 2, lines 1-19, col. 6, lines 23-48).

37. As per claim 31, Bowman discloses the content receiver, wherein the first decryption information includes a category key (col. 1, lines 12-22).

### ***Conclusion***

38. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

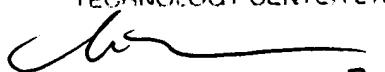
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza

AU 2136

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
4/16/07